BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Keamanan informasi menjadi kunci utama dalam sebuah sistem informasi. Masih banyak pengelola sistem informasi yang kurang memperhatikan aspek keamanan. Tidak bisa dipungkiri ada berapa sistem yang memiliki celah kerentanan dan berisiko terjadi serangan(Taufiq, 2017). Keamanan informasi merupakan upaya untuk mencegah kebocoran data dalam sistem. Untuk mengetahui celah kerentanan pada sebuah situs web harus dilakukan pengujian kerentanan pada sebuah situs web. Hasil dari evaluasi kerentanan nantinya dapat memberikan rekomendasi perbaikan kepada pengelola terhadap kerentanan yang ditemukan.

Media Informasi semakin berkembang, salah satunya penggunaan situs web. Situs web menjadi media penyampaian informasi dapat dengan mudah diakses oleh siapa saja. Universitas Jenderal Achmad Yani Yogyakarta memiliki situs web yang sering diakses oleh mahasiswa yaitu *pordik.unjaya.ac.id*. Prodik unjaya sendiri terdapat banyak informasi mengenai profil mahasiswa, Kartu Rencana Studi, Laporan Hasil Studi, Laporan keuangan. Sampai saat ini pada saat mengakses situs web pordik unjaya, selalu muncul "*Not secure*" disebelah domain *http://pordik.unjaya.ac.id* pada browser yang digunakan mengakses. Dikhawatirkan kelemahan tersebut dimanfaatkan untuk mengambil data-data penting didalamnya. Berdasarkan temuan permasalahan sebelumnya dan hasil wawancara dengan pengelola situs web pordik unjaya, bahwa penilain kerentanan pada situs web prodik unjaya belum pernah dilakukan sesuai standar pengujian, maka harus dilakukan penilaian kerentanan terhadap situs web pordik unjaya, untuk menetahui celah kerentanan apa saja yang mungkin ada pada sistem web pordik unjaya.

Tersedianya beberapa metodologi yang disediakan untuk melakukan Penilaian kerentanan, namun dari sekian banyak metode yang tersedia, pemilihan metode merupakan salah salah satu hal yang berpengaruh penting terhadap

terlaksananya tujuan kita untuk menemukan celah kerentanan. Dalam proses penilaian kerentanan ada beberapa metode yang paling banyak digunakan seperti *Information System Security Framework* (ISSAF), OWASP versi 4 dan OSSTMM. Pada penelitian ini, metode asesment yang digunakan adalah Information System Security Assessment Framework (ISSAF). Metode ISSAF dipilih karena bersifat *open source*, dan proses penilaian kerentanan terstruktur secara rinci. Dalam mencari celah kerentanan dalam sebuah situs web, ada dua tahapan yang dapat digunakan yaitu dengan *penetration testing* dan *vulnerability identification*. *Penetration testing* sendiri adalah percobaan eksploitasi sebuah situs web, sedangkan *Vulnerability Identification* lebih fokus ke penilaian kerentanan dengan proses *scanning* menggunakan tools secara otomatis. Dalam penelitian ini peneliti menggunakan *information system security assessment framework* (ISSAF), yang berfokus pada penilaian kerentanan (*vulnerability identification*)(Hariyadi et al., 2020). Dengan *Vulnerability Identification* ini nantinya akan mengetahui hasil proses scanning yang telah dilakukan.

Berdasarkan uraian permasalahan diatas maka penelitian ini ingin mengkaji mengenai "ANALISIS KERENTANAN PADA PORDIK.UNJAYA.AC.ID MENGGUNAKAN INFORMATION SYSTEM SECURITY ASSESSMENT FRAMEWORK". Tujuan penelitian ini adalah untuk mengetahui celah kerentanan situs web berdasarkan pada *vulnerability identification* dengan Framework ISSAF, sehingga bosa diberikan rekomendasi untuk meningkatkan kemanan situs web prodik unjaya nantinya.

1.2 PERUMUSAN MASALAH

Melihat latar belakang yang telah dijelaskan maka rumusan masalah dari penelitian ini adalah sebagai berikut:

1. Selalu muncul "*Not secure*" di sebelah domain pada saat mengakses pada browser.
2. Berdasarkan hasil wawancara dengan pengelola pada situs web prodik unjaya belum pernah dilakukan penilian kerentanan sesuai dengan standar pengujian.

1.3 PERTANYAAN PENELITIAN

1. Bagaimana mengidentifikasi kerentanan sistem pada situs web Pordik Unjaya?
2. Bagaimana hasil penilaian dan analisis kerentanan pada situs web Pordik Unjaya?
3. Bagaimana cara mengatasi kerentanan yang ditemukan terhadap hasil dari penilaian kerentanan yang telah dilakukan?

1.4 TUJUAN PENELITIAN

1. Mengidentifikasi kerentanan pada situs web Pordik Unjaya.
2. Mengetahui hasil penilaian dan analisis kerentanan pada domain pordik.unjaya.ac.id dengan menggunakan *Information System Security Framework* (ISSAF).
3. Mengetahui rekomendasi solusi dari temukan celah kerentanan dari hasil pengujian yang telah dilakukan.

1.5 MANFAAT HASIL PENELITIAN

Adapun manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:

1. Bagi Universitas Jenderal Achmad Yani Yogyakarta:
   a. Dapat mengidentifikasi celah kerentanan pada situs web Prodik Unjaya.
   b. Dapat mengetahui hasil penilaian dan analisis kerentanan pada situs web Prodik Unjaya dengan menggunakan *information system security framework* (ISSAF).
   c. Dapat menjadi bahan masukan kepada pengelola situs web Pordik Unjaya untuk meningkatkan sistem keamanan.
2. Bagi penulis:
   1. Dapat mengaplikasikan ilmu yang telah diperoleh selama perkuliahan di Prodi Teknologi Informasi.
   2. Dapat menambah ilmu pengetahuan serta wawasan mengenai penilaian kerentanan (*Vulnerability Identification*) sebuah situs web.